PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-111835
(43)Date of publication of application : 28.04.1998

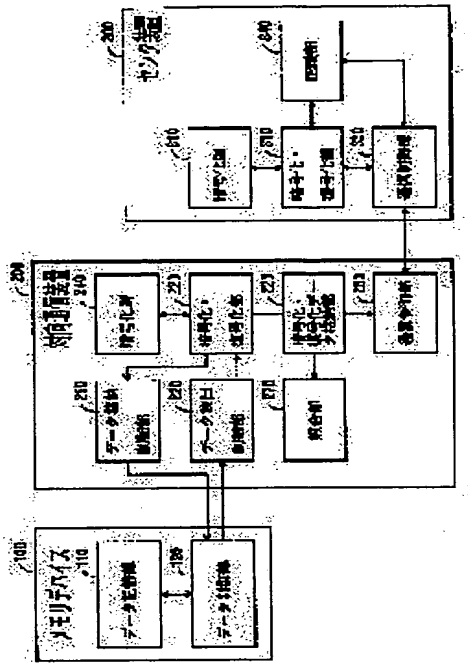
(51)Int.Cl. G06F 12/14
G06F 12/00

(21)Application number : 08-264606
(22)Date of filing : 04.10.1996

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : SAKIDA KAZUTAKA
SHIMADA IKUKO
ISHIGURO GINYA

(54) METHOD AND SYSTEM FOR IN-USE DEVICE ID TRANSMISSION

(57)Abstract:
PROBLEM TO BE SOLVED: To correctly transfer and manage an ID without receiving an illegal information report, etc., by applying a ciphering rule having a parameter to an opposite communication device and ciphering data, and writing the ciphered data and parameter in a memory device.
SOLUTION: The opposite communication device 200 ciphers data including the memory device ID of the memory device 100 as a written object according to the ciphering rule 240 having the parameter and transfers the data to the memory device 100 from a data storage control part 210. The memory device 100 stores the data in a data storage part 110. Then when the opposite communication device 200 writes to the memory device 100 thereafter, a data read control part 220 transfers a readout command and the memory device 100 extracts the ciphered data from the parameter and transfers them. The opposite communication device 200 deciphers the data by using the ciphering rule 240 and specifies the ID of the memory device 100.



LEGAL STATUS

[Date of request for examination] 11.01.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平１０－１１１８３５

(43)公開日　平成１０年（１９９８）４月２８日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
G06F 12/14	320		G06F 12/14	320 B	
12/00	510		12/00	510 A	

審査請求　未請求　請求項の数１３　ＯＬ　（全２４頁）

(21)出願番号　特願平８－２６４６０６

(22)出願日　平成８年（１９９６）１０月４日

(71)出願人　０００００４２２６
日本電信電話株式会社
東京都新宿区西新宿三丁目１９番２号

(72)発明者　崎田　一貴
東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

(72)発明者　嶋田　郁子
東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

(72)発明者　石黒　銀矢
東京都新宿区西新宿三丁目１９番２号　日本電信電話株式会社内

(74)代理人　弁理士　伊東　忠彦

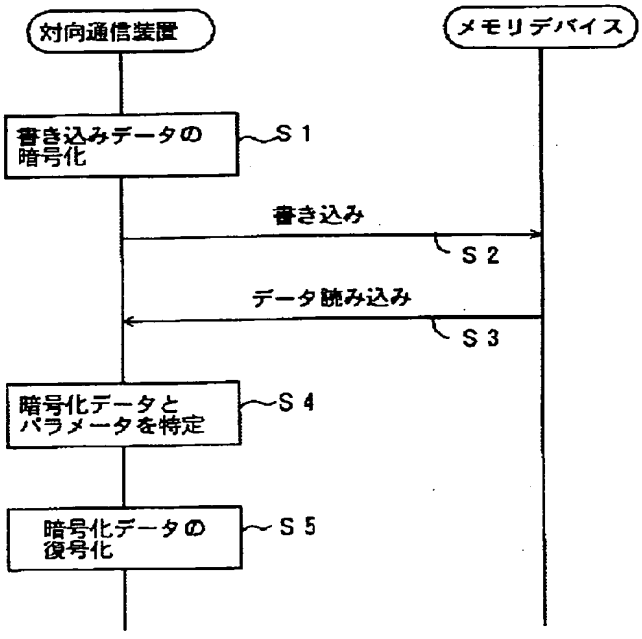
(54)【発明の名称】使用装置ＩＤ伝達方法及びシステム

(57)【要約】

【課題】　各メモリデバイス毎にそのＩＤ情報と何らかの運用履歴情報を追跡管理する必要がある時に、ＩＤ管理等を不正情報通知等を受けることなく、正しくやり取りし、管理することが可能な使用装置ＩＤ伝達方法及びシステムを提供する。

【解決手段】　本発明は、メモリデバイスＩＤを含むデータをパラメータを有する暗号化則を適用してデータを暗号化し、暗号化されたデータとパラメータをメモリデバイスに書き込み、メモリデバイスからデータを読み込んで、暗号化されたデータとパラメータを特定し、パラメータを有する暗号化則を適用して読み込んだデータを復号化する。

本発明の原理を説明するための図



1

【特許請求の範囲】

【請求項１】　複数のメモリデバイスと複数の対向通信装置及びセンタ装置及び通信回線設備から構成されるシステムにおける、使用デバイスＩＤや使用対向通信装置ＩＤを追跡管理するために該ＩＤを伝達する使用装置ＩＤ伝達方法において、

前記メモリデバイスに該メモリデバイスＩＤを含むデータを書き込む際に、前記対向通信装置においてパラメータを有する暗号化則適用してデータを暗号化し、

暗号化されたデータと前記パラメータを前記メモリデバイスに書き込み、

前記メモリデバイスからデータを読み込む際に、該メモリデバイスからデータを読み込んで、暗号化されたデータと前記パラメータを特定し、

前記パラメータを有する暗号化則を適用して読み込んだ前記データを復号化することを特徴とする使用装置ＩＤ伝達方法。

【請求項２】　前記メモリデバイスに最初にデータを書き込む第１の対向通信装置が、前記メモリデバイスＩＤを含むデータをパラメータを含む暗号化則で暗号化して、該パラメータと暗号化されたデータを該メモリデバイスに書き込み、

それ以降にデータを書き込む第２の対向通信装置が、前記メモリデバイスからデータを読み込んで、前記パラメータと前記暗号化されたデータとを抽出し、

前記暗号化されたデータを前記パラメータを有する暗号化則で復号し、メモリデバイスＩＤを特定した後、該メモリデバイスＩＤを含むデータを、パラメータを有する暗号化則で暗号化して、該パラメータと暗号化されたデータを該メモリデバイスに書き込み、

前記センタ装置が、前記メモリデバイスに書き込まれていた前記データをそのままの形式か、もしくは対向通信装置が変形した形式で、対向通信装置から通信回線を介して受け取り、受信データから暗号化データと前記暗号化則のパラメータを抽出し、該暗号化データをパラメータを有する暗号化則で復号して、前記メモリデバイスＩＤを特定する請求項１記載の使用装置ＩＤ伝達方法。

【請求項３】　前記メモリデバイスに最初にデータを書き込む第１の対向通信装置が、

書き込み対象のメモリデバイスのメモリデバイスＩＤと対向通信装置ＩＤを含むデータを、パラメータを有する暗号化側で暗号化して、該パラメータと暗号化データを該メモリデバイスに書き込み、

それ以降にデータを書き込む第２の対向通信装置が、

前記メモリデバイスからデータを読み込んで、該パラメータと前記暗号化データをパラメータを有する暗号化側で復号して、該メモリデバイスＩＤと前記第１の対向通信装置の使用対向通信装置ＩＤを特定した後、該メモリデバイスＩＤと該第２の対向通信装置の対向通信装置ＩＤを含むデータを、パラメータを有する暗号化側で暗号化し、該パラメータと暗号化データを該メモリデバイスに書き込み、

センタ装置が、

前記メモリデバイスに書き込まれていた前記データを、そのままの形式か、もしくは、前記対向通信装置が変形した形式で対向通信装置から通信回線を介して受け取り、受信データから暗号化データと暗号化側のパラメータを抽出し、該暗号化データを該パラメータを有する暗号化側で復号して、該メモリデバイスＩＤと該対向通信装置ＩＤを特定する請求項２記載の使用装置ＩＤ伝達方法。

【請求項４】　前記対向通信装置間で暗号化の第２のパラメータ、もしくは第２の暗号化則を共有し、

前記メモリデバイスに最初にデータを書き込む第１の対向通信装置が、

該メモリデバイスＩＤを前記第２のパラメータもしくは、前記第２の暗号化則で暗号化し、

暗号化された暗号化情報を含むデータを更に、第１のパラメータ若しくは、第１の暗号化則で暗号化して前記メモリデバイス内に書き込み、

それ以降にデータを書き込む第２の対向通信装置が、

前記メモリデバイスからデータを読み込んで、暗号化データを抽出し、該暗号化データを復号して、取得した該メモリデバイスＩＤと該メモリデバイスＩＤを前記第２のパラメータもしくは、前記第２の暗号化則で暗号化した情報を含むデータを特定した後、該特定されたデータを更に、前記第２のパラメータもしくは前記第２の暗号化則で復号して該メモリデバイスＩＤを特定し、２種類得られた該メモリデバイスＩＤを照合する請求項２記載の使用装置ＩＤの伝達方法。

【請求項５】　前記メモリデバイスに最初にデータを書き込む第１の対向通信装置が、

該メモリデバイスが記憶する金額情報を含むカウンタ情報を有するデータと暗号化情報を該メモリデバイス内に書き込み、

それ以降にデータを書き込む第２の対向通信装置が、

前記メモリデバイスからデータを読み込んで、前記金額情報を含むカウンタ情報と暗号化データを抽出し、さらに、該暗号化データを復号して、該金額情報を含むカウンタ情報を特定し、２種類得られた該金額情報を含むカウンタ情報を照合する請求項２記載の使用装置ＩＤ伝達方法。

【請求項６】　複数のメモリデバイスと複数の対向通信装置、センタ装置及び通信回線設備を有するシステムにおける、使用デバイスＩＤや使用対向通信装置ＩＤを追跡管理するために、該使用デバイスＩＤや該使用対向通信装置ＩＤを伝達する使用装置ＩＤ伝達システムであって、

前記メモリデバイスは、

前記対向通信装置の書き込み動作によりデータを記憶す

るデータ記憶手段を有し、
前記対向通信装置は、
書き込み対象のメモリデバイスＩＤを含むデータを暗号化したデータと、該暗号化のためのパラメータを書き込みデータとして前記メモリデバイスに書き込む書き込み手段と、
前記メモリデバイスから前記メモリデバイスＩＤを含むデータを暗号化したデータと該暗号化のパラメータを読み込みデータとして読み込むデータ読み込み手段と、
前記センタ装置と情報交信するセンタ交信手段と、
パラメータに応じて暗号化側を変化させて、暗号化、復号化すべき前記メモリデバイスＩＤを含むデータを暗号化、復号化する第１の暗号化・復号化手段と、
前記センタ装置は、
前記対向通信装置と情報交信する対向通信装置交信手段と、
前記対向通信装置交信手段と交信する交信情報から前記メモリデバイスＩＤを含むデータを暗号化したデータとその暗号化パラメータを読み込む読み込み手段と、
前記パラメータに応じて、暗号化側を変化させて前記メモリデバイスＩＤを含むデータを暗号化・復号化する第２の暗号化・復号化手段とを有することを特徴とする使用装置ＩＤ伝達システム。
【請求項７】　前記対向通信装置の前記書き込み手段は、
前記メモリデバイスに書き込むデータとして、当該メモリデバイスのメモリデバイスＩＤと自対向通信装置ＩＤを含むデータを暗号化したデータと暗号化に用いる暗号化パラメータを設定する書き込みデータ設定手段を有し、
前記データ読み込み手段は、
前記メモリデバイスから読み込むデータとして当該メモリデバイスのメモリデバイスＩＤと自対向通信装置ＩＤを含むデータを暗号化したデータと該暗号化に用いられた暗号化パラメータを設定する読み出しデータ設定手段を有し、
前記センタ装置の前記読み込み手段は、
前記対向通信装置と交信した情報から前記メモリデバイスＩＤと対向通信装置ＩＤを含むデータを暗号化した暗号化データと、暗号化の際に用いられた暗号化パラメータを読み込む手段を有し、
前記第１の暗号化・復号化手段及び前記第２の暗号化・復号化手段は、
前記メモリデバイスＩＤと前記対向通信装置ＩＤを含むデータを暗号化・復号化する手段を有する請求項６記載の使用装置ＩＤ伝達システム。
【請求項８】　前記対向通信装置は、
前記対向通信装置間で、暗号化の第２のパラメータもしくは、第２の暗号化則を共有する第２の暗号化則共有手段と、
前記第２の暗号化則共有手段において、共有されている前記第２のパラメータもしくは、前記第２の暗号化則で暗号化、復号化する第３の暗号化・復号化手段と、
前記メモリデバイスＩＤを前記第３の暗号化・復号化手段で暗号化したデータを含むデータを、更に、前記第１の暗号化・復号化手段で暗号化して、前記メモリデバイスに格納する暗号化データ格納制御手段と、
前記暗号化格納制御手段により前記メモリデバイスに格納された暗号化データを読み取る暗号化データ読み取り手段と、
前記暗号化データ読み取り手段により取得した前記暗号化データから、２種類以上の前記メモリデバイスＩＤを照合する照合手段とを有する請求項６記載の使用装置ＩＤ伝達システム。
【請求項９】　前記照合手段は、
前記暗号化データ読み取り手段により取得した暗号化データに、前記第１の暗号化・復号化手段を適用して特定した前記メモリデバイスＩＤと、同時に特定される該メモリデバイスＩＤが前記第３の暗号化・復号化手段で暗号化されている部分のデータについて更に、該第３の暗号化・復号化手段を適用して特定した前記メモリデバイスＩＤとを照合する手段を含む請求項８記載の使用装置ＩＤ伝達システム。
【請求項１０】　前記照合手段において、前記メモリデバイスＩＤが照合できた場合には、前記暗号化データ及び該メモリデバイスＩＤを暗号化したデータと暗号化パラメータを該メモリデバイスＩＤに対応する前記メモリデバイスに格納する第１の再格納手段を含む請求項９記載の使用装置ＩＤ伝達システム。
【請求項１１】　前記対向通信装置は、
金額情報を含むカウンタ情報を有するデータと該データの暗号化情報を前記メモリデバイスに格納する暗号化情報格納制御手段と、
前記暗号化情報格納制御手段により前記メモリデバイスに格納された前記カウンタ情報及び前記暗号化情報を読み取る暗号化情報読み取り手段と、
前記暗号化情報読み取り手段により取得した２種類以上の前記カウンタ情報を照合するカウンタ情報照合手段とを含む請求項６記載の使用装置ＩＤ伝達システム。
【請求項１２】　前記カウンタ情報照合手段は、
前記暗号化情報読み取り手段により取得したカウンタ情報と、前記暗号化情報を復号して特定されたカウンタ情報とを照合する手段を含む請求項１１記載の使用装置ＩＤ伝達システム。
【請求項１３】　前記カウンタ情報照合手段において、前記カウンタ情報が照合できた場合には、該カウンタ情報、メモリデバイスＩＤと該カウンタ情報を暗号化したデータ、及び暗号化パラメータをメモリデバイスＩＤに対応するメモリデバイスに格納する第２の再格納手段を含む請求項１２記載の使用装置ＩＤ伝達システム。

5

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、使用装置ＩＤ伝達方法及びシステムに係り、特に、メモリデバイスと対向通信装置、及びセンタ装置からなるシステムにおいて、使用したメモリデバイスＩＤもしくは、使用したメモリデバイスＩＤを対向通信装置及びセンタ装置が管理し、そのＩＤ管理情報から偽造メモリデバイスの使用やメモリデイバスに成り済ます行為を検知するための使用装置ＩＤ伝達方法及びシステムに関する。

【０００２】

【従来の技術】複数のメモリデバイスを用いて運用するシステムの中には、各メモリデバイス毎にそのＩＤと何らかの運用履歴情報を追跡管理する必要のあるものが存在する。これらのシステムでは、各メモリデバイスから当該メモリデバイスのＩＤと付帯情報を対向通信装置あるいは、センタ装置に通知している。このとき、当該メモリデバイスのＩＤが外部から容易に覗くことが可能で、改ざんされたり、当該ＩＤ相当に成り済まされたりすると、管理システムの機能を果たせない恐れがある。このため、通知されるＩＤの正当性が保証されることが重要である。この点を考慮して、メモリデバイスのＩＤを暗号化して通知したり、ＩＤにディジタル署名を添付して通知したり、あるいは、それらを併用したりする方法が採られている。

【０００３】

【発明が解決しようとする課題】しかしながら、上記のメモリデバイスで暗号化を行う場合は、当該デバイスに相応の演算能力やデータ記憶量等の計算リソースが必要になり、対向通信装置のみで暗号化を行う場合でも、当該デバイスに相応のデータ記憶量が必要になる。ＩＤにディジタル署名を添付する場合は、更に大量のデータ記憶量が必要になる。コスト要求条件からメモリデバイスにこれらのリソースを装備し得ないシステムでは、従来、デバイスのＩＤを直接やり取りする場合が多い。

【０００４】しかし、ＩＤを直接やりとりする方法では、ＩＤが外部から容易に覗くことができるため、ＩＤ管理システムは不正情報通知等を受け易い。また、システム構築や運用に際し、上記の危険性は無視できないので、上記の危険性はシステム構築や運用の制限条件となる。

【０００５】一方、メモリデバイスのＩＤを暗号化してやりとりする方法を採れば、上記の不正情報通知等の可能性が低くなるものの、デバイスのＩＤの暗号化を行い、暗号化されたＩＤをやりとりする方法を採った場合でも簡易な暗号化規則を採用したり、全システム共通の鍵を用いて暗号化する場合が殆どであるため、複数の情報をモニタして暗号則を推定し、然る後に、不正情報通知等を受ける可能性がある。また、暗号化規則が簡易な場合には、暗号化規則を推定され易い。また、暗号化規則を標準レベルまで複雑にしても、全システム共通の鍵を用いてしまうと、大量の情報をモニタされた場合に、暗号則を推定される恐れがある。

6

【０００６】本発明は、上記の点に鑑みなされたもので、上記従来の問題点を解決し、メモリデバイスとその対向通信装置及びセンタ装置とからなるシステムにおいて、各メモリデバイス毎にそのＩＤ情報と何らかの運用履歴情報を追跡管理する必要がある時に、ＩＤ管理等を不正情報通知等を受けることなく、正しくやり取りし、管理することが可能な使用装置ＩＤ伝達方法及びシステムを提供することを目的とする。

【０００７】

【課題を解決するための手段】図１は、本発明の原理を説明するための図である。第１の発明は、複数のメモリデバイスと複数の対向通信装置及びセンタ装置及び通信回線設備から構成されるシステムにおける、使用デバイスＩＤや使用対向通信装置ＩＤを追跡管理するために該ＩＤを伝達する使用装置ＩＤ伝達方法において、メモリデバイスにメモリデバイスＩＤを含むデータを書き込む際に、対向通信装置において、パラメータを有する暗号化則を適用してデータを暗号化し（ステップ１）、暗号化されたデータとパラメータをメモリデバイスに書き込み（ステップ２）、メモリデバイスからデータを読み込んで（ステップ３）、暗号化されたデータとパラメータを特定し（ステップ４）、パラメータを有する暗号化則を適用して読み込んだデータを復号化する（ステップ５）。

【０００８】第２の発明は、メモリデバイスに最初にデータを書き込む第１の対向通信装置が、メモリデバイスＩＤを含むデータを、パラメータを含む暗号化則で暗号化して、該パラメータと暗号化されたデータを該メモリデバイスに書き込み、それ以降にデータを書き込む第２の対向通信装置が、メモリデバイスからデータを読み込んで、パラメータと暗号化されたデータとを抽出し、暗号化されたデータをパラメータを有する暗号化則で復号し、メモリデバイスＩＤを特定した後、該メモリデバイスＩＤを含むデータを、パラメータを有する暗号化則で暗号化して、該パラメータと暗号化されたデータを該メモリデバイスに書き込み、センタ装置が、メモリデバイスに書き込まれていたデータをそのままの形式か、もしくは対向通信装置が変形した形式で、対向通信装置から通信回線を介して受け取り、受信データから暗号化データと暗号化則のパラメータを抽出し、該暗号化データをパラメータを有する暗号化則で復号して、メモリデバイスＩＤを特定する。

【０００９】第３の発明は、メモリデバイスに最初にデータを書き込む第１の対向通信装置が、書き込み対象のメモリデバイスのメモリデバイスＩＤと対向通信装置ＩＤを含むデータを、パラメータを有する暗号化側で暗号化して、該パラメータと暗号化データを該メモリデバイ

スに書き込み、それ以降にデータを書き込む第２の対向通信装置が、メモリデバイスからデータを読み込んで、該パラメータと暗号化データをパラメータを有する暗号化側で復号して、該メモリデバイスＩＤと第１の対向通信装置の使用対向通信装置ＩＤを特定した後、該メモリデバイスＩＤと該第２の対向通信装置の対向通信装置ＩＤを含むデータを、パラメータを有する暗号化側で暗号化し、該パラメータと暗号化データを該メモリデバイスに書き込み、センタ装置が、メモリデバイスに書き込まれていたデータを、そのままの形式か、もしくは、対向通信装置が変形した形式で対向通信装置から通信回線を介して受け取り、受信データから暗号化データと暗号化側のパラメータを抽出し、該暗号化データを該パラメータを有する暗号化側で復号して、該メモリデバイスＩＤと該対向通信装置ＩＤを特定する。

【００１０】第４の発明は、対向通信装置間で暗号化の第２のパラメータ、もしくは第２の暗号化則を共有し、メモリデバイスに最初にデータを書き込む第１の対向通信装置が、該メモリデバイスＩＤを第２のパラメータもしくは、第２の暗号化則で暗号化し、暗号化された暗号化情報を含むデータを更に、第１のパラメータ若しくは、第１の暗号化則で暗号化してメモリデバイス内に書き込み、それ以降にデータを書き込む第２の対向通信装置が、メモリデバイスからデータを読み込んで、暗号化データを抽出し、該暗号化データを復号して、取得した該メモリデバイスＩＤと該メモリデバイスＩＤを第２のパラメータもしくは、第２の暗号化則で暗号化した情報を含むデータを特定した後、該特定データを更に、第２のパラメータもしくは第２の暗号化則で復号して該メモリデバイスＩＤを特定し、２種類得られた該メモリデバイスＩＤを照合する。

【００１１】第５の発明は、メモリデバイスに最初にデータを書き込む第１の対向通信装置が、該メモリデバイスが記憶する金額情報を含むカウンタ情報を有するデータと暗号化情報を該メモリデバイス内に書き込み、それ以降にデータを書き込む第２の対向通信装置が、メモリデバイスからデータを読み込んで、金額情報を含むカウンタ情報と暗号化データを抽出し、さらに、該暗号化データを復号して、該金額情報を含むカウンタ情報を特定し、２種類得られた該金額情報を含むカウンタ情報を照合する。

【００１２】図２は、本発明の原理構成図である。第６の発明は、複数のメモリデバイス１００と複数の対向通信装置２００、センタ装置３００及び通信回線設備４００を有するシステムにおける、使用デバイスＩＤや使用対向通信装置ＩＤを追跡管理するために、該使用デバイスＩＤや該使用対向通信装置ＩＤを伝達する使用装置ＩＤ伝達システムであって、メモリデバイス１００は、対向通信装置２００の書き込み動作によりデータを記憶するデータ記憶手段１１０を有し、対向通信装置２００は、書き込み対象のメモリデバイスＩＤを含むデータを暗号化したデータと、該暗号化のためのパラメータを書き込みデータとしてメモリデバイスに書き込む書き込み手段２１０と、メモリデバイス１００からメモリデバイスＩＤを含むデータを暗号化したデータと該暗号化のパラメータを読み込みデータとして読み込むデータ読み込み手段２２０と、センタ装置３００と情報交信するセンタ交信手段２５０と、パラメータに応じて暗号化側を変化させて、暗号化、復号化すべきメモリデバイスＩＤを含むデータを暗号化、復号化する第１の暗号化・復号化手段２３０と、センタ装置３００は、対向通信装置と情報交信する対向通信装置交信手段３３０と、対向通信装置交信手段３３０と交信する交信情報からメモリデバイスＩＤを含むデータを暗号化したデータとその暗号化パラメータを読み込む読み込み手段３４０と、パラメータに応じて、暗号化側を変化させてメモリデバイスＩＤを含むデータを暗号化・復号化する第２の暗号化・復号化手段３１０とを有する。

【００１３】第７の発明において、対向通信装置２００の書き込み手段２１０は、メモリデバイス１００に書き込むデータとして、当該メモリデバイス１００のメモリデバイスＩＤと自対向通信装置ＩＤを含むデータを暗号化したデータと暗号化に用いる暗号化パラメータを設定する書き込みデータ設定手段を有し、データ読み込み手段２２０は、メモリデバイス１００から読み込むデータとして当該メモリデバイス１００のメモリデバイスＩＤと自対向通信装置ＩＤを含むデータを暗号化したデータと該暗号化に用いられた暗号化パラメータを設定する読み出しデータ設定手段を有し、センタ装置３００の読み込み手段３４０は、対向通信装置と交信した情報から、メモリデバイスＩＤと対向通信装置ＩＤを含むデータを暗号化した暗号化データと、暗号化の際に用いられた暗号化パラメータを読み込む手段を有し、第１の暗号化・復号化手段及び第２の暗号化・復号化手段３１０は、メモリデバイスＩＤと対向通信装置ＩＤを含むデータを暗号化・復号化する手段を有する。

【００１４】第８の発明において、対向通信装置２００は、対向通信装置２００間で、暗号化の第２のパラメータもしくは、第２の暗号化則を共有する第２の暗号化則共有手段と、第２の暗号化則共有手段において、共有されている第２のパラメータもしくは、第２の暗号化則で暗号化、復号化する第３の暗号化・復号化手段と、メモリデバイスＩＤを第３の暗号化・復号化手段で暗号化したデータを含むデータを、更に、第１の暗号化・復号化手段で暗号化して、メモリデバイス１００に格納する暗号化データ格納制御手段と、暗号化格納制御手段によりメモリデバイス１００に格納された暗号化データを読み取る暗号化データ読み取り手段と、暗号化データ読み取り手段により取得した暗号化データから、２種類以上のメモリデバイスＩＤを照合する照合手段とを有する。

9

【００１５】第９の発明において、照合手段は、暗号化データ読み取り手段により取得した暗号化データに、第１の暗号化・復号化手段を適用して特定したメモリデバイスＩＤと、同時に特定される該メモリデバイスＩＤが第３の暗号化・復号化手段で暗号化されている部分のデータについて更に、該第３の暗号化・復号化手段を適用して特定したメモリデバイスＩＤとを照合する手段を含む。

【００１６】第１０の発明は、照合手段において、メモリデバイスＩＤが照合できた場合には、暗号化データとメモリデバイスＩＤに対応するメモリデバイスＩＤを暗号化したデータ及び暗号化パラメータをメモリデバイス１００に格納する第１の再格納手段を含む。

【００１７】第１１の発明において、対向通信装置２００は、金額情報を含むカウンタ情報を有するデータと該データの暗号化情報を該メモリデバイス１００に格納する暗号化情報格納制御手段と、暗号化情報格納制御手段によりメモリデバイス１００に格納されたカウンタ情報及び暗号化情報を読み取る暗号化情報読み取り手段と、暗号化情報読み取り手段により取得した２種類以上のカウンタ情報を照合するカウンタ情報照合手段とを含む。

【００１８】第１２の発明において、カウンタ情報照合手段は、暗号化情報読み取り手段により取得したカウンタ情報と、暗号化情報を復号して、特定されたカウンタ情報とを照合する手段を含む。第１３の発明は、カウンタ情報照合手段において、カウンタ情報が照合できた場合には、該カウンタ情報、メモリデバイスＩＤと該カウンタ情報を暗号化したデータ、及び暗号化パラメータを格納する第２の再格納手段を含む。

【００１９】上記の第１、第２の発明は、メモリデバイスに当該メモリデバイスのＩＤ（メモリデバイスＩＤ）を含むデータを書き込む際に、パラメータを有する暗号化則を適用してデータを暗号化し、当該暗号化データとパラメータをメモリデバイスＩＤに対応する当該メモリデバイスに書き込む。さらに、メモリデバイスからデータを読み込む際には、メモリデバイスからデータを読み込んで、暗号化データとパラメータを特定し、パラメータを有する暗号化則を適用してデータを復号することにより、共有鍵を用いずに各メモリデバイス固有のパラメータを用いて暗号化・復号化が可能となる。

【００２０】第３の発明は、第１、第２の発明におけるメモリデバイスＩＤを含むデータの書き込み、読み込みの代わりに、対向通信装置がメモリデバイスＩＤと対向通信装置ＩＤを含むデータの書き込み、読み込みを行うことにより、さらに複雑化した暗号化・復号化が可能となる。

【００２１】第４の発明は、第１、第２の発明における方法に加えて、対向通信装置間で暗号化の別のパラメータを共有し、対向通信装置がメモリデバイスＩＤを別のパラメータで暗号化した情報を含めたデータを更に暗号化して、メモリデバイスに書き込み、かつ、当該メモリデバイスから読み出して復号する。別のパラメータで暗号化された部分については、更に復号し、この２つの手順により取得したメモリデバイスＩＤを照合することにより、照合できない場合には不正であると判定することが可能となる。

10

【００２２】第５の発明は、第１、第２の発明における方法に加えて、対向通信装置が金額情報等のカウンタ情報をメモリデバイスに書き込むと共に、カウンタ情報を含むデータを暗号化して書き込み、かつ、メモリデバイスから読み出して復号し、２つのカウンタ情報を照合することにより、照合できない場合には不正であると判定することが可能となる。

【００２３】第６の発明は、対向通信装置とセンタ装置に、パラメータに応じて暗号化則を変化させてデータを暗号化、復号する手段を設け、メモリデバイスのメモリデバイスＩＤを含むデータを暗号化したデータと、暗号化のパラメータをメモリデバイス内に書き込むことにより、対向通信装置とセンタ装置においてメモリデバイス固有の鍵情報を取得し、暗号化・復号化が可能となる。

【００２４】第７の発明は、第６の発明におけるメモリデバイスＩＤを含むデータを暗号化したデータと暗号化パラメータをメモリデバイスに書き込む代わりに、メモリデバイスＩＤと対向装置ＩＤを含むデータを暗号化したデータと、暗号化パラメータをメモリデバイス内に記録することにより、複雑化した暗号化・復号化が必要となるため、容易に復号化して悪用することが困難となる。

【００２５】第８、第９及び第１０の発明は、第６の発明に加え、対向通信装置に対向通信装置間で暗号化のための別のパラメータを共有させることにより、対向通信装置及びセンタ装置に、メモリデバイスのＩＤを別のパラメータで暗号化及び復号化する手段を設け、さらに、２種類のメモリデバイスＩＤを照合することにより、照合できない場合には、不正であるものと判定することができる。

【００２６】第１１、第１２及び第１３の発明は、第６の発明に加え、対向通信装置にメモリデバイスに金額情報等のカウンタ情報を書き込む手段と、カウンタ情報を含むデータを暗号化して書き込む手段と、メモリデバイスからデータを読み出して復号し、カウンタ情報を特定する手段と、暗号化されたカウンタ情報を復号し、特定されているカウンタ情報の２種類のカウンタ情報を照合する手段を設けることにより、２つのカウンタ情報を照合して、照合できない場合には、不正であるものと判定することができる。

【００２７】このように、本発明は、各メモリデバイスに、必要情報の暗号化データに加え、当該各メモリデバイス固有の暗号化パラメータを含めて記録できるので、各対向通信装置及びセンタ装置が暗号化パラメータから

各メモリデバイス固有の鍵情報を導出することができる。このため、当該鍵情報を用いて、暗号化、復号化が実施できる。これにより、メモリデバイスに演算能力やデータ記憶量等の計算リソースを過大に持たせることなく、当該メモリデバイスのＩＤ情報等を各メモリデバイス毎に異なる暗号化パラメータで暗号化して通知することができ、不正情報通知等を受け難いＩＤ管理システムが実現できる。

【００２８】さらに、メモリデバイスに、当該メモリデバイスのＩＤ情報を別のパラメータで暗号化したデータに加えて暗号化して書き込み、当該メモリデバイスから読み出して復号する時に、２種のＩＤ情報を照合することにより、暗号化、復号化処理の正当性を推定することができる。

【００２９】また、メモリデバイスに金額情報等のカウンタ情報を書き込むと共に、カウンタ情報を含むデータを暗号化して書き込み、メモリデバイスから読み出して２つのカウンタ情報を復号した結果、２つのカウンタ情報を照合することにより、カウンタ情報の改ざんを抑止できる。

【００３０】

【発明の実施の形態】図３は、本発明の第１の使用装置ＩＤ伝送システムの構成を示す。同図に示すシステムは、メモリデバイス１００、対向通信装置２００、センタ装置３００、及び対向通信装置２００とセンタ装置３００を接続する通信回線設備４００より構成される。

【００３１】同図に示す例は、メモリデバイス１００と対向通信装置２００は、直接交信する形態の例である。対向通信装置２００が、メモリデバイス１００にコマンドを発行すると、メモリデバイス１００が、応答し、アクセスを許可する。これにより、対向通信装置２００は、コマンドを介してメモリデバイス１００にデータを書き込むことができる。

【００３２】図４は、本発明の使用装置ＩＤ伝送システムの各装置構成を示す。メモリデバイス１００は、対向通信装置２００からのコマンドに従いデータを記憶するデータ記憶部１１０と、対向通信装置２００からのコマンドに従い、データ書き込み要求または、読み込み要求に応じて、データ記憶部１１０を制御して、対向通信装置２００からの要求に対応する制御を行うデータ制御部１２０より構成される。

【００３３】対向通信装置２００は、メモリデバイス１００にデータを書き込むコマンドを発行し、データ転送を行うデータ格納制御部２１０、メモリデバイス１００からデータを取得するコマンドを発行し、データの読み込みを行うデータ読出制御部２２０、パラメータに応じて暗号化則を変化させてデータを暗号化・復号化する暗号化・復号化部２３０、データを暗号化・復号化するための規則である暗号化則２４０、及びセンタ装置３００と情報交信する通信制御部２５０、暗号化・復号化部２３０により暗号化・復号化されたデータを格納する暗号化・復号化データ格納部２６０、復号化された２種類以上のメモリデバイスＩＤや金額情報等のカウンタ情報を照合する照合部２７０より構成される。

【００３４】センタ装置３００は、パラメータに応じて暗号化則を変化させてデータを暗号化・復号化する暗号化・復号化部３１０、暗号化・復号化部３１０により参照される暗号化則３２０、対向通信装置２００と情報を交信する通信制御部３３０、暗号化・復号化された情報、または、転送されたデータからメモリデバイスＩＤ、対向通信装置ＩＤを認識する認識部３４０から構成される。

【００３５】上記の構成において、対向通信装置２００が最初にデータを書き込む装置である場合には、暗号化・復号化部２３０において、書き込み対象のメモリデバイス１００のメモリデバイスＩＤを含むデータを、パラメータを有する暗号化則２４０で暗号化してデータ格納制御部２１０に転送する。これにより、データ格納制御部２１０は、当該暗号化データをメモリデバイス１００に転送する。メモリデバイス１００のデータ制御部１２０は、当該暗号化データをデータ記憶部１１０に格納する。

【００３６】また、対向通信装置２００が上記の対向通信装置以降（ｎ番目：ｎ≧２）にメモリデバイス１００に書き込みを行う装置である場合には、対向通信装置２００のデータ読出制御部２２０がメモリデバイス１００に読出用のコマンドを転送する。メモリデバイス１００のデータ制御部１２０が当該コマンドを受け取ると、データ記憶部１１０からパラメータと暗号化データを抽出し、対向通信装置２００のデータ読出制御部２２０に転送する。これにより、転送されたデータは、読出制御部２２０から暗号化・復号化部２３０に転送される。暗号化・復号化部２３０は、暗号化データを抽出し、暗号化則２４０を用いて復号して、メモリデバイス１００のメモリデバイスＩＤを特定する。更に、当該メモリデバイスＩＤを暗号化則２４０を用いて暗号化して、当該暗号化則２４０のうち、暗号化に用いられたパラメータと暗号化されたメモリデバイスＩＤを暗号化データとして、データ格納制御部２１０を介してメモリデバイス１００に転送する。これにより、当該データがメモリデバイス１００のデータ制御部１２０を介してデータ記憶部１１０に格納される。

【００３７】さらに、本発明では、最初にメモリデバイス１００に書き込みを行う対向通信装置２００がメモリデバイスＩＤと自装置２００の対向通信装置ＩＤを暗号化則２４０を用いて暗号化・復号化部２３０で暗号化して、メモリデバイス１００のデータ記憶部１１０に書き込む。さらに、ｎ番目にメモリデバイス１００に書き込みを行う対向通信装置２００は、メモリデバイス１００から暗号化データを読み出して、暗号化則２４０を用い

て暗号化・復号化部２３０で当該データを復号し、メモリデバイスＩＤとｎ－１番目または、ｎ－ｉ（ｎ＞ｉ≧２）番目にメモリデバイス１００に書き込みを行った対向通信装置２００の対向通信装置ＩＤを特定し、暗号化則２４０の暗号化パラメータを用いて、対向通信装置ＩＤとメモリデバイスＩＤを暗号化・復号化部２３０で暗号化して、データ格納制御部２１０を介してメモリデバイス１００のデータ記憶部１１０に書き込む。

【００３８】さらに、本発明では、対向通信装置２００は、上記のようにして得られたメモリデバイスＩＤ（Ａ）を暗号化・復号化データ格納部２６０に格納しておくと共に、当該メモリデバイスＩＤを暗号化則２４０の他のパラメータで暗号化し、当該暗号化されたメモリデバイスＩＤを復号したメモリデバイスＩＤ（Ｂ）を暗号化・復号化データ格納部２６０に格納する。これにより、最初に格納されたメモリデバイスＩＤ（Ａ）と次に格納されたメモリデバイスＩＤ（Ｂ）を照合部２７０に転送し、当該照合部２７０で両者が一致するかを調べる。

【００３９】さらに、本発明では、対向通信装置２００（１）は、金額情報等のカウンタ情報を含むデータと暗号化情報をメモリデバイス１００のデータ格納部１１０に書き込み、それ以降にメモリデバイス１００に書き込みを行う対向通信装置（ｎ）が、メモリデバイス１００からデータを読み込んで、カウンタ情報と暗号化情報を抽出して暗号化・復号化データ格納部２６０に格納しておき、当該暗号化情報を復号し、カウンタ情報を特定し、暗号化・復号化データ格納部２６０に格納されているカウンタ情報と復号されたカウンタ情報を照合部２７０で照合する。

【００４０】また、センタ装置３００は、メモリデバイス１００のデータ記憶部１１０に書き込まれていたデータをそのままの形式、または、対向通信装置２００により変形された形式で、通信制御部３３０を介して取得し、暗号化データを暗号化則３２０を用いて暗号化・復号化部３１０で復号して、復号されたデータを認識部３４０に転送し、データ認識部３４０でメモリデバイス１００を特定する。

【００４１】また、センタ装置３００は、暗号化データに対向通信装置ＩＤも含まれている場合には、暗号化・復号化部３１０で復号してメモリデバイス１００と対向通信装置２００を特定する。また、上記の構成は、メモリデバイス１００と対向通信装置２００が直接交信する構成であるが、図５に示すように、通信回線設備４００を介してメモリデバイス１００と対向通信装置２００が交信する形態がある。

【００４２】図５に示す構成は、対向通信装置は、物理的な対向通信装置２０１と論理的な対向通信装置２０２があり、物理的な対向通信装置２０１は単なる中継装置としてのみ働き、前述の対向通信装置が行う処理は、全て論理的な対向通信装置２０２が行う。論理的な対向通信装置２０２とセンタ装置３００は、通信回線設備４００を介して接続されており、相互に通信可能である。

【００４３】

【実施例】以下、図面と共に本発明の実施例を説明する。

［第１の実施例］第１の実施例として、第１の対向通信装置がメモリデバイスに暗号化されたデータ（メモリデバイスＩＤ）を書き込み、第２の対向通信装置が第１の対向通信装置により書き込まれたデータを復号し、さらに、独自に暗号化したデータをメモリデバイスに書き込み、センタ装置において、対向通信装置から渡されたデータを特定する例を示す。

【００４４】図６は、本発明の第１の実施例の処理の概要を示す。同図において、メモリデバイス１００ａと最初にやり取りする対向通信装置２００ａは、メモリデバイス１００ａのＩＤを含むデータを暗号化したデータαとその暗号化パラメータαを、メモリデバイス１００ａの指定レコード位置に書き込む。以降、メモリデバイス１００ａとやり取りする対向通信装置２００ｂは、メモリデバイス１００ａから暗号化パラメータαを読み取り、暗号化データ復号則を推定する。暗号化パラメータから復号則を導出する方法は、正規の対向通信装置間で共有している。

【００４５】さらに、メモリデバイス１００ａから暗号化データαを読み取り、これを復号してメモリデバイスＩＤを取得する。センタ装置３００は、対向通信装置２００ｂから暗号化パラメータαを読み取り、暗号化復号則を推定する。暗号化パラメータから復号則を導出する方法は、正規の対向通信装置及びセンタ装置間で共有している。

【００４６】さらに、センタ装置３００は、対向通信装置２００ｂから暗号化データαを読み取り、これを復号してメモリデバイスＩＤを取得する。図７は、本発明の第１の実施例のメモリデバイスと対向通信装置が最初にやり取りする動作を示すフローチャートである。

【００４７】ステップ１０１）　対向通信装置２００ａは、メモリデバイス１００ａを起動させる。

ステップ１０２）　メモリデバイス１００ａが起動する。

ステップ１０３）　対向通信装置２００ａは、データを書き込むメモリデバイス１００ａのメモリデバイスＩＤを特定する。

【００４８】ステップ１０４）　対向通信装置２００ａが書き込みデータを暗号化するための暗号化パラメータαを特定する。

ステップ１０５）　対向通信装置２００ａの暗号化・復号化部２３０は、メモリデバイス１００のメモリデバイスＩＤを含むデータを暗号化則２４０の暗号化パラメータαを用いて暗号化する。

【００４９】ステップ１０６）　対向通信装置２００ａのデータ格納制御部２１０は、暗号化時に使用した暗号化パラメータαをメモリデバイス１００ａのデータ記憶部１１０の指定レコード位置に書き込むためのコマンドをメモリデバイス１００ａに送信する。

【００５０】ステップ１０７）　メモリデバイス１００ａのデータ制御部１２０は、対向通信装置２００ａから暗号化パラメータαの書き込みのコマンドを受け取ると、データ記憶部１１０の指定レコード位置に、暗号化パラメータαを書き込む。

ステップ１０８）　さらに、対向通信装置２００ａは、暗号化された暗号化データαをメモリデバイス１００ａのデータ記憶部１１０の指定レコード位置に書き込むためのコマンドをメモリデバイス１００に送信する。

【００５１】ステップ１０９）　メモリデバイス１００ａのデータ制御部１２０は、対向通信装置２００ａから暗号化データαの書き込みのコマンドを受け取ると、データ記憶部１２０の指定レコード位置に、暗号化データαを書き込む。図８は、本発明の第１の実施例のメモリデバイスと対向通信装置が２回目以降にやり取りする際の動作のフローチャートである。

【００５２】ステップ１１０）　対向通信装置２００ｂがメモリデバイス１００ａを起動する。

ステップ１１１）　メモリデバイス１００ａが起動する。

ステップ１１２）　対向通信装置２００ｂは、メモリデバイス１００ａのデータ記憶部１１０に格納されている暗号化パラメータαを読み取るコマンドをデータ読出制御部２２０から発行する。

【００５３】ステップ１１３）　メモリデバイス１００ａのデータ制御部１２０は、対向通信装置２００ｂに対して、データ記憶部１１０からの暗号化パラメータαの読み出しを許可する。

ステップ１１４）　対向通信装置２００ｂのデータ読出制御部２２０は、メモリデバイス１００ａのデータ記憶部１１０から暗号化パラメータαを読み取る。

【００５４】ステップ１１５）　次に、対向通信装置２００ｂのデータ読出制御部２２０は、メモリデバイス１００ａに対して暗号化データαを読み出すコマンドを送信する。

ステップ１１６）　メモリデバイス１００ａのデータ制御部１２０は、受信した読み出しコマンドに対する読み出しを許可する。

【００５５】ステップ１１７）　対向通信装置２００ｂのデータ読出制御部２２０は、メモリデバイス１００ａから暗号化データαを読み取り、暗号化・復号化データ格納部２６０に格納する。

ステップ１１８）　対向通信装置２００ｂのデータ読出制御部２２０により取得し、暗号化・復号化データ格納部２６０に格納されている暗号データαを暗号化・復号化部２３０により復号する。

【００５６】ステップ１１９）　復号された暗号化データαからメモリデバイス１００ａのメモリデバイスＩＤを特定する。なお、上記のステップ１１８において暗号化データを復号化する際に用いる復号化パラメータは、正規の対向通信装置間（２００ａ，２００ｂ）で共有しているものとする。

【００５７】さらに、図７に示す動作と同様に、対向通信装置２００ｂが暗号化パラメータβ、暗号化データβをメモリデバイス１００ａに転送し、メモリデバイス１００ａにおいて、当該暗号化パラメータβと暗号化データβをデータ記憶部１１０に格納する。

【００５８】図９は、本発明の第１の実施例の対向通信装置とセンタ装置の動作のフローチャートである。

ステップ１２０）　センタ装置３００は、対向通信装置２００ｂを起動させる。

【００５９】ステップ１２１）　対向通信装置２００ｂが起動する。

ステップ１２２）　センタ装置３００は、暗号化パラメータαを読み取るコマンドを通信制御部３３０を介して対向通信装置２００ｂに発行する。

ステップ１２３）　対向通信装置２００ｂは、通信制御部２５０を介して当該コマンドを受信すると、暗号化・復号化データ格納部２６０に格納されている暗号化データαを通信制御部２５０を介してセンタ装置３００に送信する。

【００６０】ステップ１２４）　センタ装置３００は、暗号化データαを通信制御部３３０を介して読み取り、暗号化・復号化部３１０に転送する。

ステップ１２５）　暗号化・復号化部３１０は、暗号化データを暗号化則３２０の暗号パラメータを用いて復号し、復号した結果を認識部３４０に転送する。

【００６１】ステップ１２６）　認識部３４０は、復号した結果よりメモリデバイスＩＤを特定する。

［第２の実施例］次に、第２の実施例として、第１の対向通信装置がメモリデバイスに暗号化されたデータ（メモリデバイスＩＤ、対向通信装置ＩＤ）を書き込み、第２の対向通信装置が第１の対向通信装置により書き込まれたデータを復号し、さらに、独自に暗号化したデータ（メモリデバイスＩＤ、対向通信装置ＩＤ）をメモリデバイスに書き込み、センタ装置において、対向通信装置から渡されたデータ（メモリデバイスＩＤ、対向通信装置ＩＤ）を特定する例を示す。

【００６２】図１０は、本発明の第２の実施例の処理の概要を示す図である。メモリデバイス１００ａと最初にやり取りする対向通信装置２００ａは、当該メモリデバイス１００ａのＩＤと対向通信装置ＩＤを含むデータを暗号化したデータγと、暗号化パラメータγを、メモリデバイス１００ａの指定レコード位置に書き込む。以降、メモリデバイス１００ａとやり取りする対向通信装

置２００ｂは、メモリデバイス１００ａから暗号化パラメータγを読み取り、暗号化データ復号則を推定する。なお、暗号化パラメータから復号則を導出する方法は、正規の対向通信装置間で共有している。

【００６３】さらに、対向通信装置２００ｂは、メモリデバイス１００ａから暗号化データγを読み取り、これを復号してメモリデバイスＩＤと前にやり取りしていた対向通信装置ＩＤを取得する。その後、メモリデバイス１００ａのＩＤと対向通信装置ＩＤを含むデータを暗号化したデータδとその暗号化パラメータδを、メモリデバイス１００ａの指定レコード位置に書き込む。

【００６４】センタ装置３００は、対向通信装置２００ｂから暗号化パラメータγを読み取り、暗号化データ復号則を推定する。なお、暗号化パラメータから復号則を導出する方法は、正規の対向通信装置及びセンタ装置間で共有している。さらに、センタ装置３００は、対向通信装置２００ｂから暗号化データγを読み取り、これを復号してメモリデバイスＩＤと前にやり取りがあった対向通信装置ＩＤを取得する。

【００６５】図１１は、本発明の第２の実施例のメモリデバイスと対向通信装置が最初にやり取りする動作を示すフローチャートである。

ステップ２０１）　対向通信装置２００ａは、メモリデバイス１００ａを起動する。

【００６６】ステップ２０２）　メモリデバイス１００ａが起動する。

ステップ２０３）　対向通信装置２００ａは、メモリデバイス１００ａのメモリデバイスＩＤを特定する。

ステップ２０４）　対向通信装置２００ａは、暗号化則２４０から暗号化パラメータγを特定する。

【００６７】ステップ２０５）　対向通信装置２００ａは、メモリデバイスＩＤと自対向通信装置２００ａの対向通信装置ＩＤを含むデータを暗号化・復号化部２３０において暗号化パラメータγを用いて暗号化する。

ステップ２０６）　対向通信装置２００ａは、暗号化パラメータγをデータ格納制御部２１０を介してメモリデバイス１００ａに書き込むためのコマンドを送信する。

【００６８】ステップ２０７）　メモリデバイス１００ａは、暗号化パラメータγをデータ記憶部１１０に書き込む。

ステップ２０８）　対向通信装置２００ａは、対向通信装置ＩＤを含む暗号化データγをメモリデバイス１００ａに書き込むためのコマンドを送信する。

【００６９】ステップ２０９）　メモリデバイス１００ａは、暗号化データγをデータ記憶部１１０に書き込む。図１２は、本発明の第２の実施例のメモリデバイスと対向通信装置が２回目以降にやり取りする際の動作のフローチャートである。

【００７０】ステップ２１０）　対向通信装置２００ｂがメモリデバイス１００ａを起動する。

ステップ２１１）　メモリデバイス１００ａが起動する。

ステップ２１２）　対向通信装置２００ｂは、メモリデバイス１００ａのデータ記憶部１１０に格納されている暗号化パラメータγを読み取るコマンドをデータ読出制御部２２０から発行する。

【００７１】ステップ２１３）　メモリデバイス１００ａのデータ制御部１２０は、対向通信装置２００ｂに対してデータ記憶部１１０からの暗号化パラメータγの読み出しを許可する。

ステップ２１４）　対向通信装置２００ｂのデータ読出制御部２２０は、メモリデバイス１００ａのデータ記憶部１１０から暗号化パラメータγを読み取る。

【００７２】ステップ２１５）　次に、対向通信装置２００ｂのデータ読出制御部２２０は、メモリデバイス１００ａに対して暗号化データγを読み出すコマンドを送信する。

ステップ２１６）　メモリデバイス１００ａのデータ制御部１２０は、受信した読み出したコマンドに対する読み出しを許可する。

【００７３】ステップ２１７）　対向通信装置２００ｂのデータ読出制御部２２０は、メモリデバイス１００ａから暗号化データγを読み取り、暗号化・復号化データ格納部２６０に格納する。

ステップ２１８）　対向通信装置２００ｂのデータ読出制御部２２０により取得し、暗号化・復号化データ格納部２６０に格納されている暗号データγを暗号化・復号化部２３０により復号する。

【００７４】ステップ２１９）　復号された暗号化データγからメモリデバイス１００ａのメモリデバイスＩＤと対向通信装置ＩＤを含むデータを特定する。

ステップ２２０）　対向通信装置２００ｂは、メモリデバイスＩＤと対向通信装置ＩＤを含むデータを、暗号化則２４０の暗号化パラメータδを用いて暗号化・復号化部２３０で暗号化する。

【００７５】ステップ２２１）　対向通信装置２００ｂは、暗号化・復号化部２３０で用いられた暗号化パラメータδをメモリデバイス１００ａに書き込むためのコマンドをデータ格納制御部２１０を介して送信する。

ステップ２２２）　メモリデバイス１００ａは、データ記憶部１１０に暗号化パラメータδを書き込む。

【００７６】ステップ２２３）　対向通信装置２００ｂは、対向通信装置ＩＤを含む暗号化データδを書き込むコマンドをデータ格納制御部２１０を介して送信する。

ステップ２２４）　メモリデバイス１００ａは、暗号化データδをデータ記憶部１１０に書き込む。

【００７７】図１３は、本発明の第２の実施例の対向通信装置とセンタ装置との動作のフローチャートである。

ステップ２３０）　センタ装置３００は、相手の対向通信装置２００ｂを起動する。

【００７８】ステップ２３１）　対向通信装置２００ｂが起動する。

ステップ２３２）　センタ装置３００は、暗号化パラメータを読み取るコマンドを通信制御部３３０から対向通信装置２００ｂに発行する。

ステップ２３３）　対向通信装置２００ｂは、暗号化・復号化データ格納部２６０に格納されている暗号化パラメータγを通信制御部２５０を介してセンタ装置３００に送信する。

【００７９】ステップ２３４）　センタ装置３００は、対向通信装置２００ｂから暗号化パラメータγを受信し、暗号化データ復号則を推定する。なお、暗号化パラメータから復号則を導く方法は、正規の対向通信装置２００及びセンタ装置３００間で共有している。

【００８０】ステップ２３５）　センタ装置３００は、暗号化データを読み取るコマンドを対向通信装置２００ｂに通信制御部３３０から発行する。

ステップ２３６）　対向通信装置２００ｂは、暗号化・復号化データ格納部２６０に格納されている暗号化データγをセンタ装置３００に送信する。

【００８１】ステップ２３７）　センタ装置３００は、対向通信装置２００ｂから暗号化データγを受信する。

ステップ２３８）　センタ装置３００の暗号化・復号化部３１０は、暗号化データγを復号し、復号結果を認識部３４０に転送する。

【００８２】ステップ２３９）　センタ装置３００の認識部３４０は、復号結果からメモリデバイスＩＤ（１００ａ）と対向通信装置ＩＤ（２００ｂ）を特定する。

［第３の実施例］次に、第３の実施例を説明する。

【００８３】図１４は、本発明の第３の実施例の処理の概要を示す。本実施例は、全ての対向通信装置２００に暗号化則と暗号化パラメータＡを共有させておき、メモリデバイス１００ａと最初のやり取りする対向通信装置２００ａが、まず、メモリデバイスのＩＤを含むデータに暗号化パラメータＡを適用して暗号化し、次に、暗号化データとメモリデバイスＩＤを含むデータに暗号化パラメータＢを適用して更に暗号化し、当該暗号化データＢと暗号化パラメータＢをメモリデバイス１００ａの指定レコード位置に格納する。以降、メモリデバイス１００ａとやり取りする対向通信装置２００ｂは、メモリデバイス１００ａから暗号化データＢ及び暗号化パラメータＢを読み取り、暗号化データ復号則を推定する。推定復号則を暗号化データＢに適用し、メモリデバイスＩＤを含むデータや当該暗号化データＢを特定する。特定した暗号化データについては、暗号化パラメータＡを適用して更に復号し、メモリデバイスＩＤを特定する。

【００８４】その結果、当該メモリデバイス１００ａのメモリデバイスＩＤが２度特定されたことになるので、２種のメモリデバイスＩＤが等しく得られたかどうか、２種のデータを照合する。その結果、照合できたとき、対向通信装置２００ｂは、メモリデバイス１００ａのメモリデバイスＩＤを取得する。

【００８５】図１５は、本発明の第３の実施例のメモリデバイスと対向通信装置が最初にデータをやり取りする動作のフローチャートである。

ステップ３０１）　対向通信装置２００ａは、メモリデバイス１００ａを起動する。

【００８６】ステップ３０２）　メモリデバイス１００ａが起動する。

ステップ３０３）　対向通信装置２００ａは、メモリデバイス１００ａのメモリデバイスＩＤを特定する。

ステップ３０４）　対向通信装置２００ａは、暗号化則２４０から暗号化パラメータＡを特定する。

【００８７】ステップ３０５）　対向通信装置２００ａの暗号化・復号化部２３０は、ステップ３０３で特定したメモリデバイスＩＤを含むデータを暗号化パラメータＡを用いて暗号化し、当該暗号化結果を暗号化データＡとする。

ステップ３０６）　対向通信装置２００ａは、暗号化則２４０から暗号化パラメータＢを特定する。

【００８８】ステップ３０７）　上記のメモリデバイスＩＤと、暗号化データＡを暗号化パラメータＢを用いて更に暗号化し、当該暗号化結果を暗号化データＢとする。

ステップ３０８）　対向通信装置２００ａは、データ格納制御部２１０を介して暗号化パラメータＢをメモリデバイス１００ａに転送する。

【００８９】ステップ３０９）　メモリデバイス１００ａのデータ制御部１２０は、対向通信装置２００ａから取得した暗号化パラメータＢをデータ記憶部１１０に格納する。

ステップ３１０）　対向通信装置２００ａは、暗号化データＢを書き込むコマンドをデータ格納制御部２１０からメモリデバイス１００ａに転送する。

【００９０】ステップ３１１）　メモリデバイス１００ａのデータ制御部１２０は、対向通信装置２００ａから取得した暗号化データＢをデータ記憶部１１０に格納する。図１６は、本発明の第３の実施例のメモリデバイスと対向通信装置が２回目以降にやり取りする際の動作のフローチャートである。

【００９１】ステップ３２０）　対向通信装置２００ｂがメモリデバイス１００ａを起動する。

ステップ３２１）　メモリデバイス１００ａが起動する。

ステップ３２２）　対向通信装置２００ｂは、暗号化パラメータＢを読み取るコマンドをデータ読出制御部２２０からメモリデバイス１００ａに発行する。

【００９２】ステップ３２３）　メモリデバイス１００ａのデータ制御部１２０は、データ記憶部１１０に格納されている暗号化パラメータＢを読み出し可能とする。

ステップ３２４）　対向通信装置２００ｂのデータ読出制御部２２０は、暗号化パラメータＢをデータ記憶部１１０から読み取る。

【００９３】ステップ３２５）　対向通信装置２００ｂは、暗号化データＢを読み取るコマンドをデータ読出制御部２２０からメモリデバイス１００ａに発行する。

ステップ３２６）　メモリデバイス１００ａのデータ制御部１２０は、データ記憶部１１０に格納されている暗号化データＢを読み出し可能とする。

【００９４】ステップ３２７）　対向通信装置２００ｂのデータ読出制御部２２０は、暗号化データＢをデータ記憶部１１０から読み取る。

ステップ３２８）　対向通信装置２００ｂの取得した暗号化データＢを暗号化パラメータＢで復号する。

【００９５】ステップ３２９）　対向通信装置２００ｂは、復号結果からメモリデバイスＩＤ、暗号化データを特定し、暗号化・復号化データ格納部２６０に格納する。

ステップ３３０）　各対向通信装置２００で共有している暗号化パラメータＡを特定する。

【００９６】ステップ３３１）　対向通信装置２００ｂは、ステップ３２７で取得した暗号化データＢを暗号化パラメータＡで復号する。

ステップ３３２）　対向通信装置２００ｂは、復号結果からメモリデバイスＩＤを特定する。

【００９７】ステップ３３３）　対向通信装置２００ｂの照合部２７０は、ステップ３２９において、暗号化・復号化データ格納部２６０に格納されているメモリデバイスＩＤとステップ３３２で特定されたメモリデバイスＩＤを照合し、照合できない場合にはステップ３３４に移行し、照合できた場合には、ステップ３３５に移行する。

【００９８】ステップ３３４）　照合失敗の所定の処理を行い、処理を終了する。

ステップ３３５）　対向通信装置２００ｂの暗号化・復号化部２２３０は、メモリデバイスＩＤと上記暗号化データＢを含むデータを更に暗号化する。

ステップ３３６）　対向通信装置２００ｂのデータ格納制御部２１０は、暗号化パラメータＢをメモリデバイス１００ａのデータ格納部１１０に格納するコマンドをメモリデバイス１００ａに送出する。

【００９９】ステップ３３７）　メモリデバイス１００ａは、データ格納部１１０に暗号化パラメータＢを格納する。

ステップ３３８）　対向通信装置２００ｂは、メモリデバイス１００ａに暗号化データを書き込むコマンドをデータ格納制御部２１０から発行する。

【０１００】ステップ３３９）　メモリデバイス１００ａは、データ記憶部１１０に暗号化データを書き込む。

［第４の実施例］図１７は、本発明の第４の実施例の処理の概要を示す図である。

【０１０１】メモリデバイス１００ａと最初のやり取りする対向通信装置２００ａは、メモリデバイス１００ａのメモリデバイスＩＤとカウンタ情報を含むデータを暗号化した暗号化データλと当該暗号化パラメータλ及びカウンタ情報をメモリデバイス１００ａのデータ記憶部１１０に書き込む。

【０１０２】以降、メモリデバイス１００ａとやり取りする対向通信装置２００ｂは、カウンタ情報をメモリデバイス１００ａから読み取ると共に、暗号化パラメータλを読み取り、暗号化データ復号則を推定する。暗号化パラメータλから復号則を導出する方法は、対向通信装置２００間で共有している。更に、メモリデバイス１００ａから暗号化データλを読み取り、これを復号して、メモリデバイス１００ａのメモリデバイスＩＤとカウンタ情報を特定する。

【０１０３】その結果、カウンタ情報が２度特定されたことになるので、２種のカウンタ情報が等しく得られたかどうか、２種のデータを照合する。照合の結果、照合できた場合には、対向通信装置２００ｂは、カウンタ情報が正当なものであると見なして取得する。

【０１０４】その後、対向通信装置２００ｂは、必要であれば、カウンタ情報を更新し、メモリデバイス１００ａのメモリデバイスＩＤとカウンタ情報を含むデータを暗号化したデータと当該暗号化パラメータ及びカウンタ情報をメモリデバイス１００ａのデータ記憶部１１０に格納する。

【０１０５】図１８は、本発明の第４の実施例のメモリデバイスと対向通信装置が最初にデータをやり取りする動作を示すフローチャートである。

ステップ４０１）　対向通信装置２００ａは、メモリデバイス１００ａを起動する。

【０１０６】ステップ４０２）　メモリデバイス１００ａが起動する。

ステップ４０３）　対向通信装置２００ａは、メモリデバイスＩＤを特定する。

ステップ４０４）　対向通信装置２００ａは、カウンタ情報を特定する。

【０１０７】ステップ４０５）　対向通信装置２００ａは、暗号化パラメータλを特定する。

ステップ４０６）　対向通信装置２００ａは、メモリデバイスＩＤとカウンタ情報を含むデータを暗号化して、暗号化データλとする。

【０１０８】ステップ４０７）　対向通信装置２００ａのデータ格納制御部２１０は、カウンタ情報をメモリデバイス１００ａのデータ記憶部１１０に格納するためのコマンドを送信する。

ステップ４０８）　メモリデバイス１００ａのメモリデバイス１００ａのデータ記憶部１１０は、対向通信装置２００ａから転送されたカウンタ情報を書き込む。

【０１０９】ステップ４０９）　対向通信装置２００ａは、暗号化パラメータλをメモリデバイス１００ａのデータ記憶部１１０に書き込むコマンドを送信する。

ステップ４１０）　メモリデバイス１００ａのメモリデバイス１００ａのデータ記憶部１１０は、対向通信装置２００ａから転送された暗号化パラメータλを書き込む。

【０１１０】ステップ４１１）　対向通信装置２００ａは、暗号化データλをメモリデバイス１００ａのデータ記憶部１１０に書き込むコマンドを送信する。

ステップ４１２）　メモリデバイス１００ａのメモリデバイス１００ａのデータ記憶部１１０は、対向通信装置２００ａから転送された暗号化データλを書き込む。

【０１１１】図１９は、本発明の第４の実施例のメモリデバイスと対向通信装置が２回目以降にやり取りする際の動作のフローチャートである。

ステップ４２０）　対向通信装置２００ｂがメモリデバイス１００ａを起動する。

【０１１２】ステップ４２１）　メモリデバイス１００ａが起動する。

ステップ４２２）　対向通信装置２００ｂは、カウンタ情報を読み取るコマンドをデータ読出制御部２２０からメモリデバイス１００ａに発行する。

ステップ４２３）　メモリデバイス１００ａのデータ制御部１２０は、データ記憶部１１０に格納されているカウンタ情報を読み出し可能とする。

【０１１３】ステップ４２４）　対向通信装置２００ｂのデータ読出制御部２２０は、カウンタ情報をデータ記憶部１１０から読み取る。

ステップ４２５）　対向通信装置２００ｂは、暗号化パラメータλを読み取るコマンドをデータ読出制御部２２０からメモリデバイス１００ａに発行する。

【０１１４】ステップ４２６）　メモリデバイス１００ａのデータ制御部１２０は、データ記憶部１１０に格納されている暗号化パラメータλを読み出し可能とする。

ステップ４２７）　対向通信装置２００ｂのデータ読出制御部２２０は、暗号化パラメータλをデータ記憶部１１０から読み取る。

【０１１５】ステップ４２８）　対向通信装置２００ｂは、暗号化データλを読み取るコマンドをデータ読出制御部２２０からメモリデバイス１００ａに発行する。

ステップ４２９）　メモリデバイス１００ａのデータ制御部１２０は、データ記憶部１１０に格納されている暗号化データλを読み出し可能とする。

【０１１６】ステップ４３０）　対向通信装置２００ｂのデータ読み出し制御部２２０は、暗号化データλをデータ記憶部１１０から読み取る。

ステップ４３１）　対向通信装置２００ｂの取得した暗号化データλを暗号化パラメータλで復号する。

【０１１７】ステップ４３２）　対向通信装置２００ｂは、復号結果からメモリデバイスＩＤ、カウンタ情報を特定し、暗号化・復号化データ格納部２６０に格納する。

ステップ４３３）　対向通信装置２００ｂは、ステップ４２４において、メモリデバイス１００ａから取得したカウンタ情報と、ステップ４３１で復号されたカウンタ情報を照合し、照合できなかった場合には、ステップ４３４に以降し、照合できた場合にはステップ４３５に移行する。

【０１１８】ステップ４３４）　照合しなかった場合には、所定の照合不可処理を行い、処理を終了する。

ステップ４３５）　対向通信装置２００ｂは、当該カウンタ情報を更新する。

ステップ４３６）　対向通信装置２００ｂの暗号化・復号化部２３０は、メモリデバイス１００ａのメモリデバイスＩＤとカウンタ情報を含むデータを暗号化する。

【０１１９】ステップ４３７）　対向通信装置２００ｂは、更新されたカウンタ情報をデータ記憶部１１０に書き込むためのコマンドをデータ格納制御部２１０を介してメモリデバイス１００ａに送信する。

ステップ４３８）　メモリデバイス１００ａのデータ記憶部１１０は、更新されたカウンタ情報を格納する。

【０１２０】ステップ４３９）　対向通信装置２００ｂは、暗号化パラメータを書き込むコマンドをデータ格納制御部２１０を介してメモリデバイス１００ａに送出する。

ステップ４４０）　メモリデバイス１００ａのデータ記憶部１１０は、暗号化パラメータをデータ記憶部１１０に書き込む。

【０１２１】ステップ４４１）　対向通信装置２００ｂは、暗号化データを書き込むコマンドをデータ格納制御部２１０を介してメモリデバイス１００ａに送出する。

ステップ４４２）　メモリデバイス１００ａのデータ記憶部１１０は、暗号化データをデータ記憶部１１０に書き込む。

【０１２２】なお、本発明は、上記の実施例の限定されることなく、特許請求の範囲内で種々変更・応用が可能である。

【０１２３】

【発明の効果】上述のように、本発明の使用装置ＩＤ伝達方法及びシステムによれば、メモリデバイスに演算能力やデータ記憶量等の計算リソースを過大に持たせることなく、不正情報通知等を受け難いＩＤ管理システムが実現できる。

【０１２４】また、本発明によれば、照合処理を行うことにより、暗号化、復号化処理の正当性が推定でき、金額情報等のカウンタ情報の改ざんを防止することが可能である。

【図面の簡単な説明】

【図１】本発明の原理を説明するための図である。

25　　26

【図２】本発明の原理構成図である。

【図３】本発明の第１の使用装置ＩＤ伝送システムの構成図である。

【図４】本発明の使用装置ＩＤ伝送システムの各装置構成図である。

【図５】本発明の第２の使用装置ＩＤ伝送システムの構成図である。

【図６】本発明の第１の実施例の処理の概要を示す図である。

【図７】本発明の第１の実施例のメモリデバイスと対向通信装置が最初のデータをやり取りする動作を示すフローチャートである。

【図８】本発明の第１の実施例のメモリデバイスと対向通信装置が２回目以降にやり取りする際の動作のフローチャートである。

【図９】本発明の第１の実施例の対向通信装置とセンタ装置との動作のフローチャートである。

【図１０】本発明の第２の実施例の処理の概要を示す図である。

【図１１】本発明の第２の実施例のメモリデバイスと対向通信装置が最初にやり取りする動作のフローチャートである。

【図１２】本発明の第２の実施例のメモリデバイスと対向通信装置が２回目以降にやり取りする際の動作のフローチャートである。

【図１３】本発明の第２の実施例の対向通信装置とセンタ装置との動作のフローチャートである。

【図１４】本発明の第３の実施例の処理の概要を示す図である。

【図１５】本発明の第３の実施例のメモリデバイスと対向通信装置が最初にデータをやり取りする動作のフローチャートである。

【図１６】本発明の第３の実施例のメモリデバイスと対向通信装置が２回目以降にやり取りする際の動作のフローチャートである。

【図１７】本発明の第４の実施例の処理の概要を示す図である。

【図１８】本発明の第４の実施例のメモリデバイスと対向通信装置が最初にやり取りする動作を示すフローチャートである。

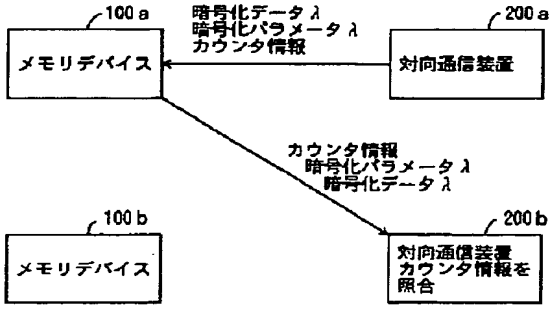
【図１９】本発明の第４の実施例のメモリデバイスと対向通信装置が２回目以降にやり取りする際の動作のフローチャートである。

【符号の説明】

１００　メモリデバイス
１１０　データ記憶部、データ記憶手段
１２０　データ制御部
２００　対向通信装置
２０１　物理的な対向通信装置
２０２　論理的な対向通信装置
２１０　データ格納制御部、書き込み手段
２２０　データ読出制御部、読み込み手段
２３０　暗号化・復号化部、第１の暗号化・復号化手段
２４０　暗号化則
２５０　通信制御部、センタ交信手段
２６０　暗号化・復号化データ格納部
２７０　照合部
３００　センタ装置
３１０　暗号化・復号化部、第２の暗号化・復号化手段
３２０　暗号化則
３３０　通信制御部、対向通信装置交信手段
３４０　認識部、読み込み手段
４００　通信回線設備

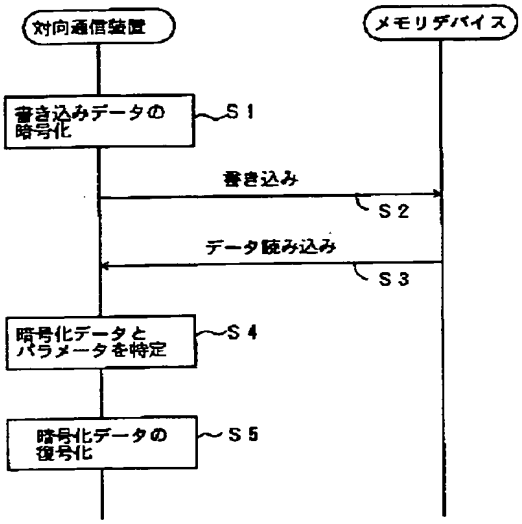
【図１７】

本発明の第４の実施例の処理の概要を示す図



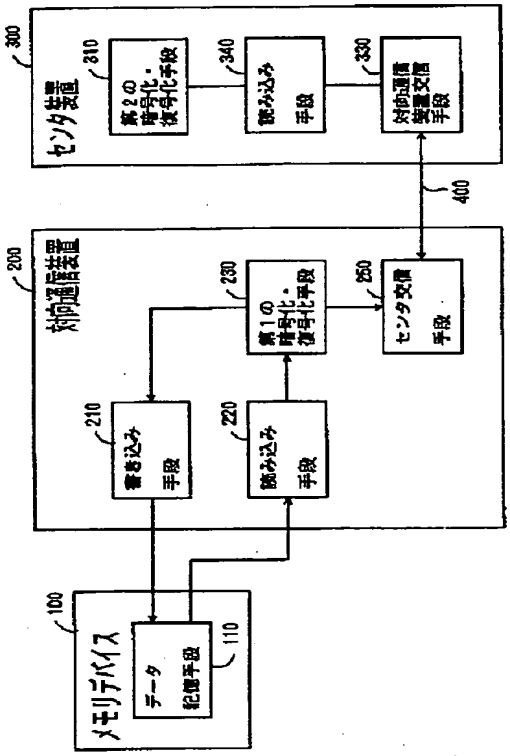
【図１】

本発明の原理を説明するための図



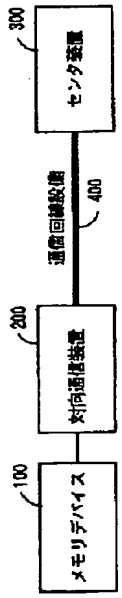
【図２】

本発明の原理構成図



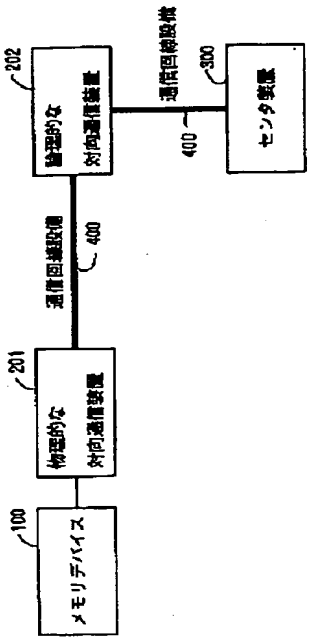
【図３】

本発明の第１の使用装置ＩＤ伝送システムの構成図



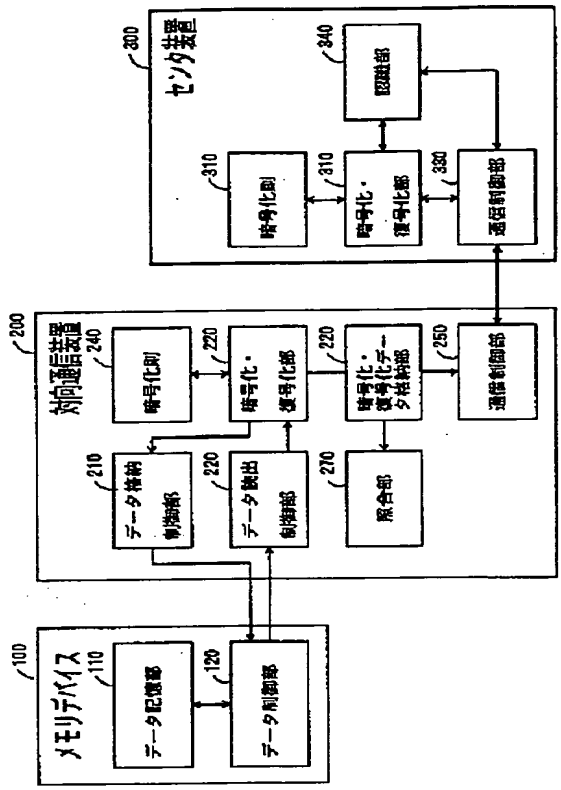
【図５】

本発明の第２の使用装置ＩＤ伝送システムの構成図



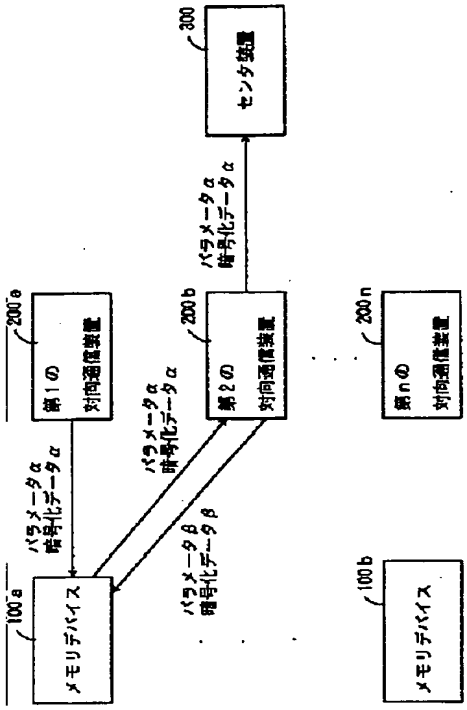
【図４】

本発明の使用装置ＩＤ伝送システムの各装置構成図



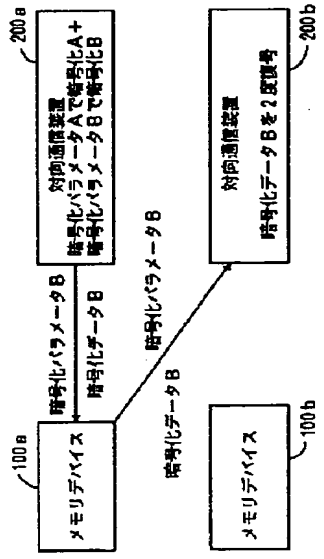
【図６】

本発明の第１の実施例の処理の概要を示す図



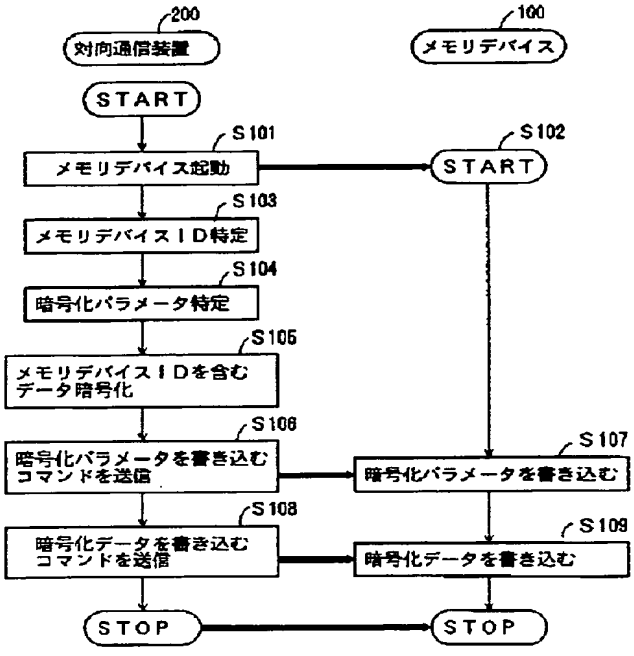
【図１４】

本発明の第３の実施例の処理の概要を示す図



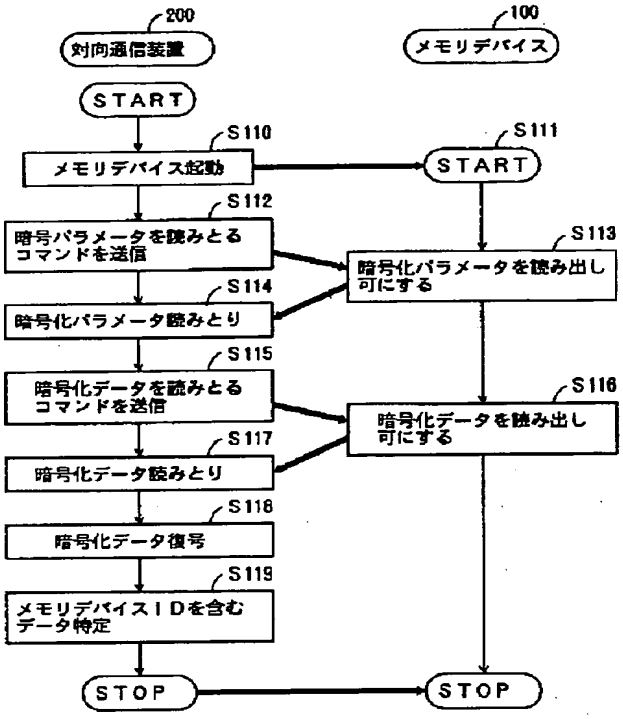
【図７】

本発明の第１の実施例のメモリデバイスと対向通信装置が最初にデータをやり取りする動作を示すフローチャート



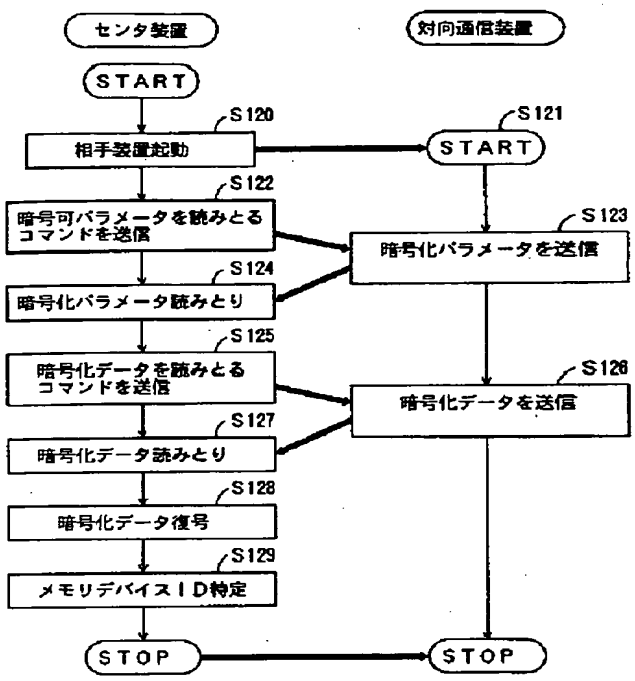
【図８】

本発明の第１の実施例のメモリデバイスと対向通信装置が２回目以降にデータをやり取りする動作を示すフローチャート



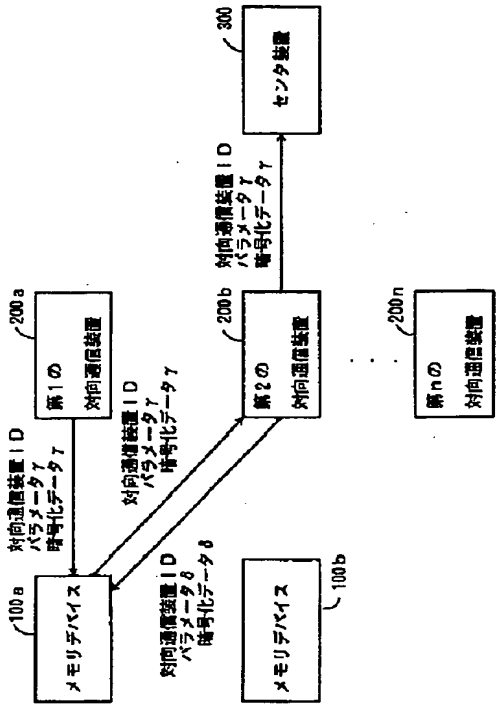
【図９】

本発明の第１の実施例の対向通信装置とセンタ装置との動作のフローチャート



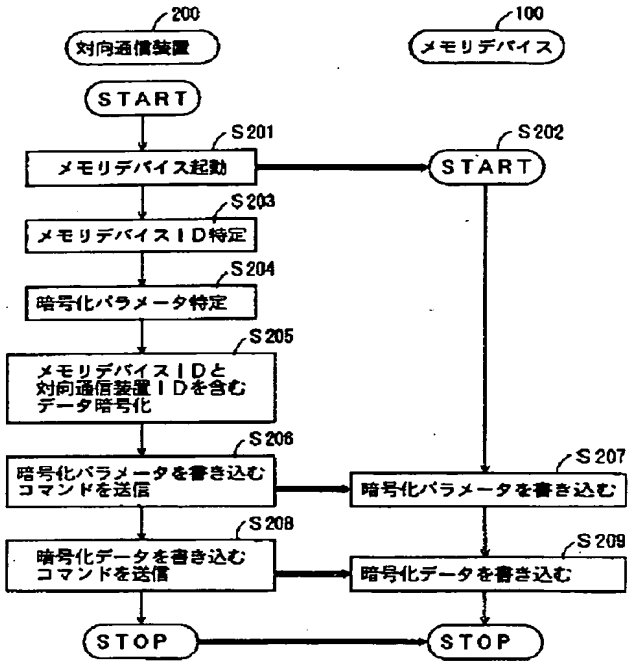
【図１０】

本発明の第２の実施例の処理の概要を示す図



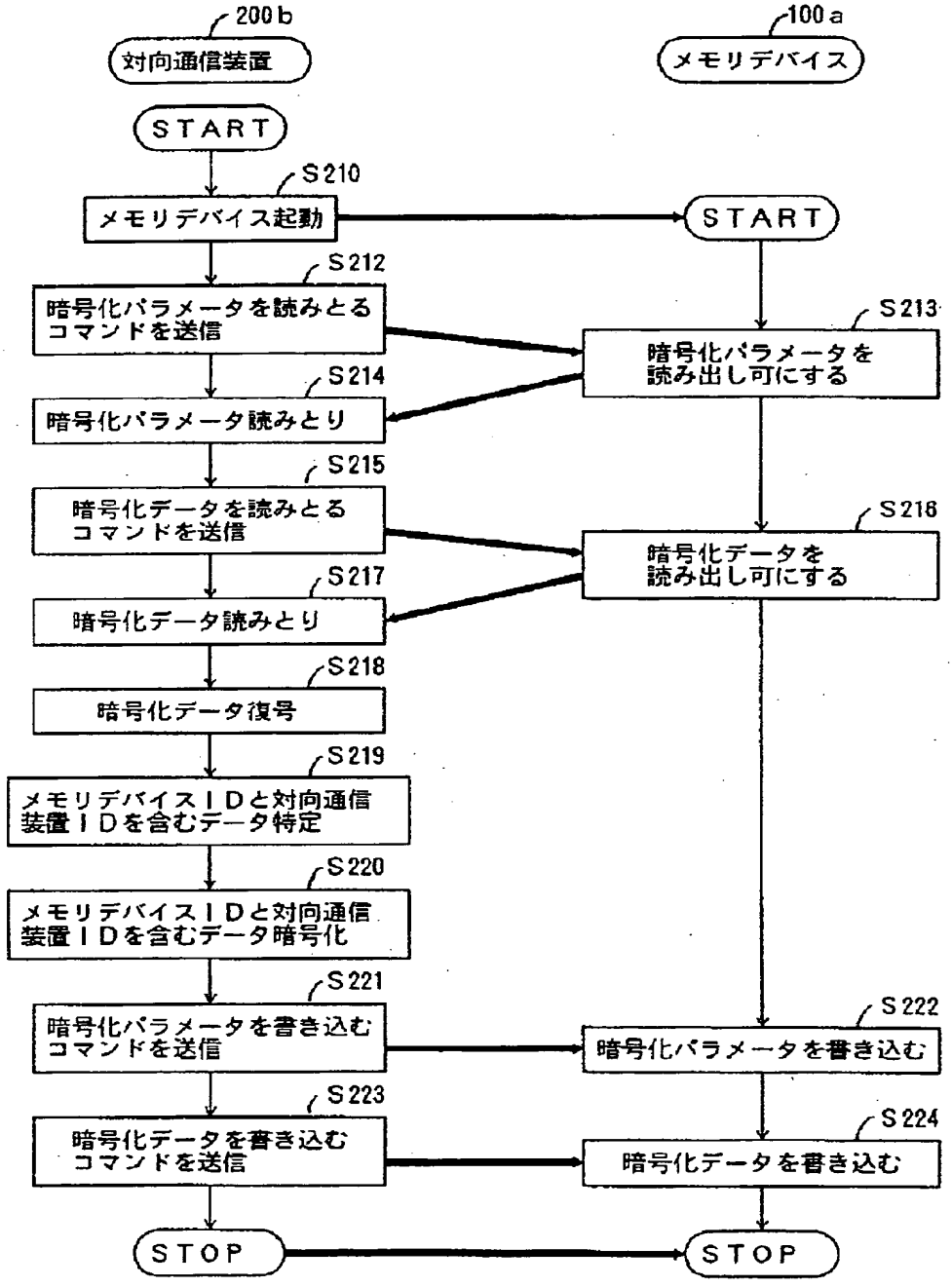
【図１１】

本発明の第２の実施例のメモリデバイスと対向通信装置が最初にデータをやり取りする動作を示すフローチャート



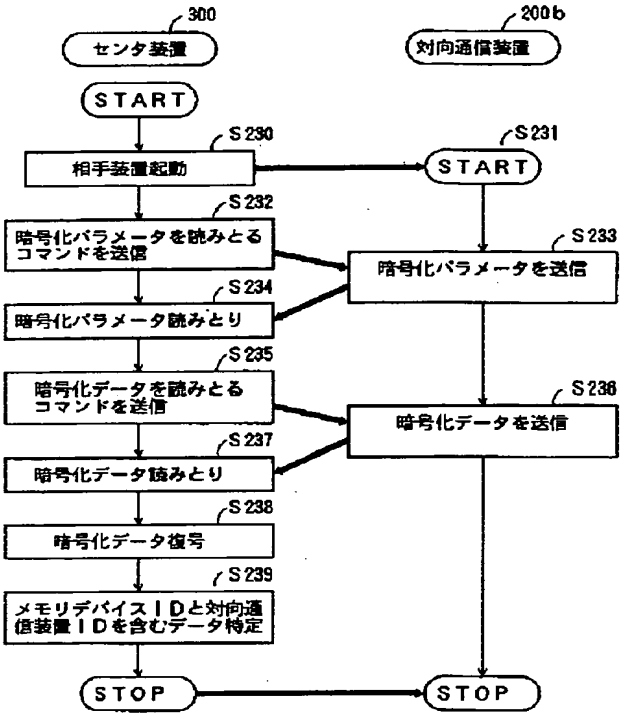
【図１２】

本発明の第２の実施例のメモリデバイスと対向通信装置が２回目以降にやり取りする際の動作のフローチャート



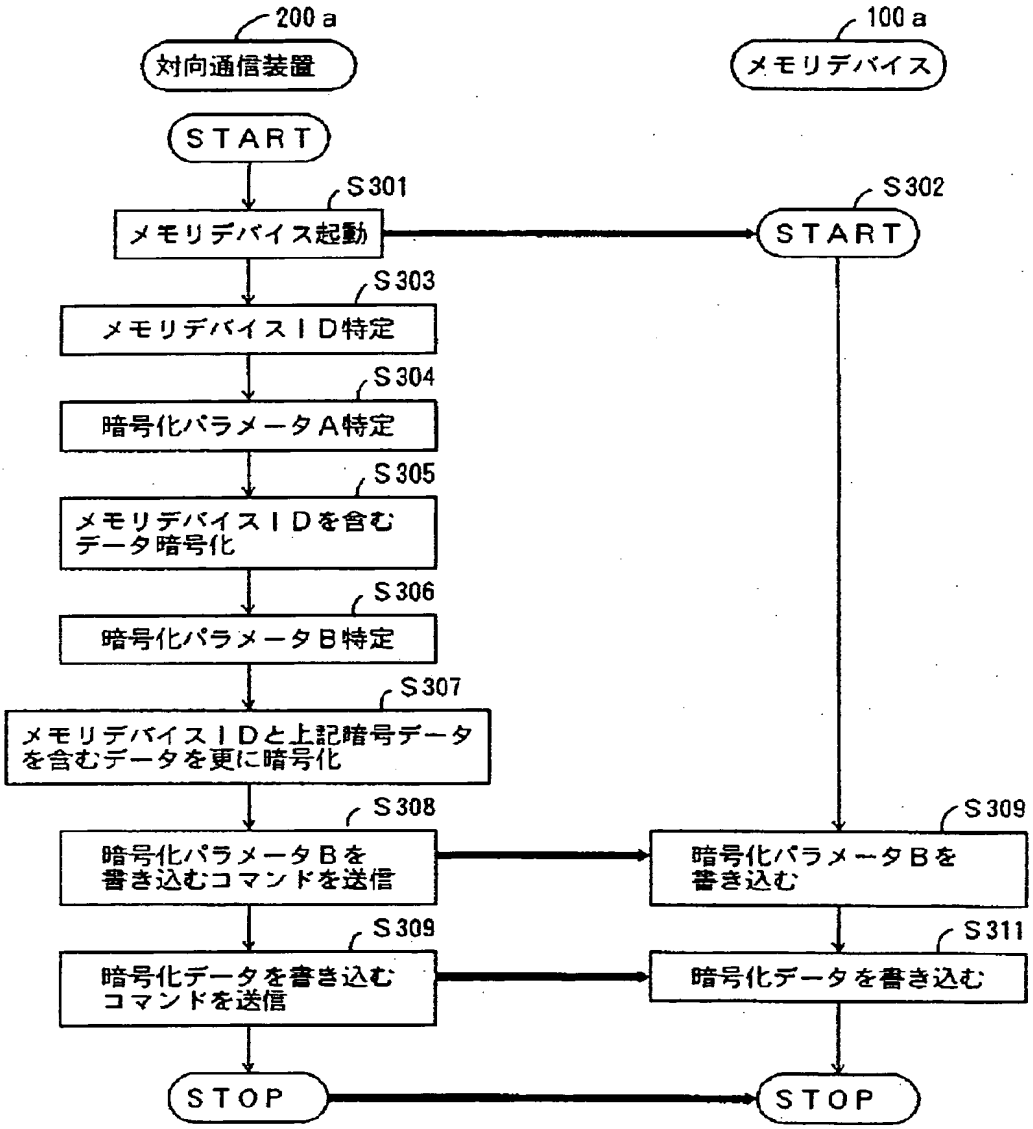
【図１３】

本発明の第２の実施例の対向通信装置と
センタ装置との動作のフローチャート



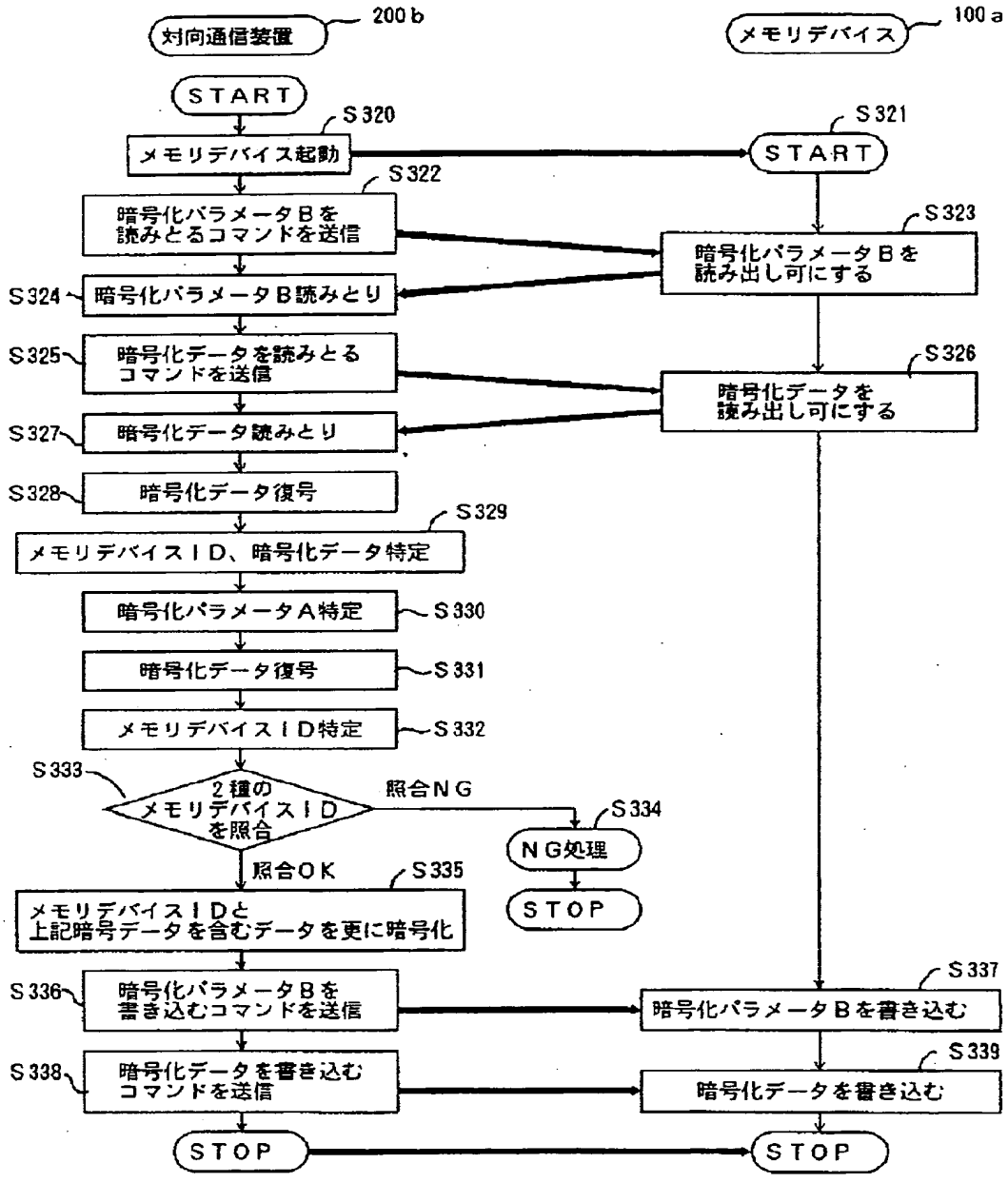
【図１５】

本発明の第３の実施例のメモリデバイスと対向通信装置が最初にデータをやり取りする際の動作のフローチャート



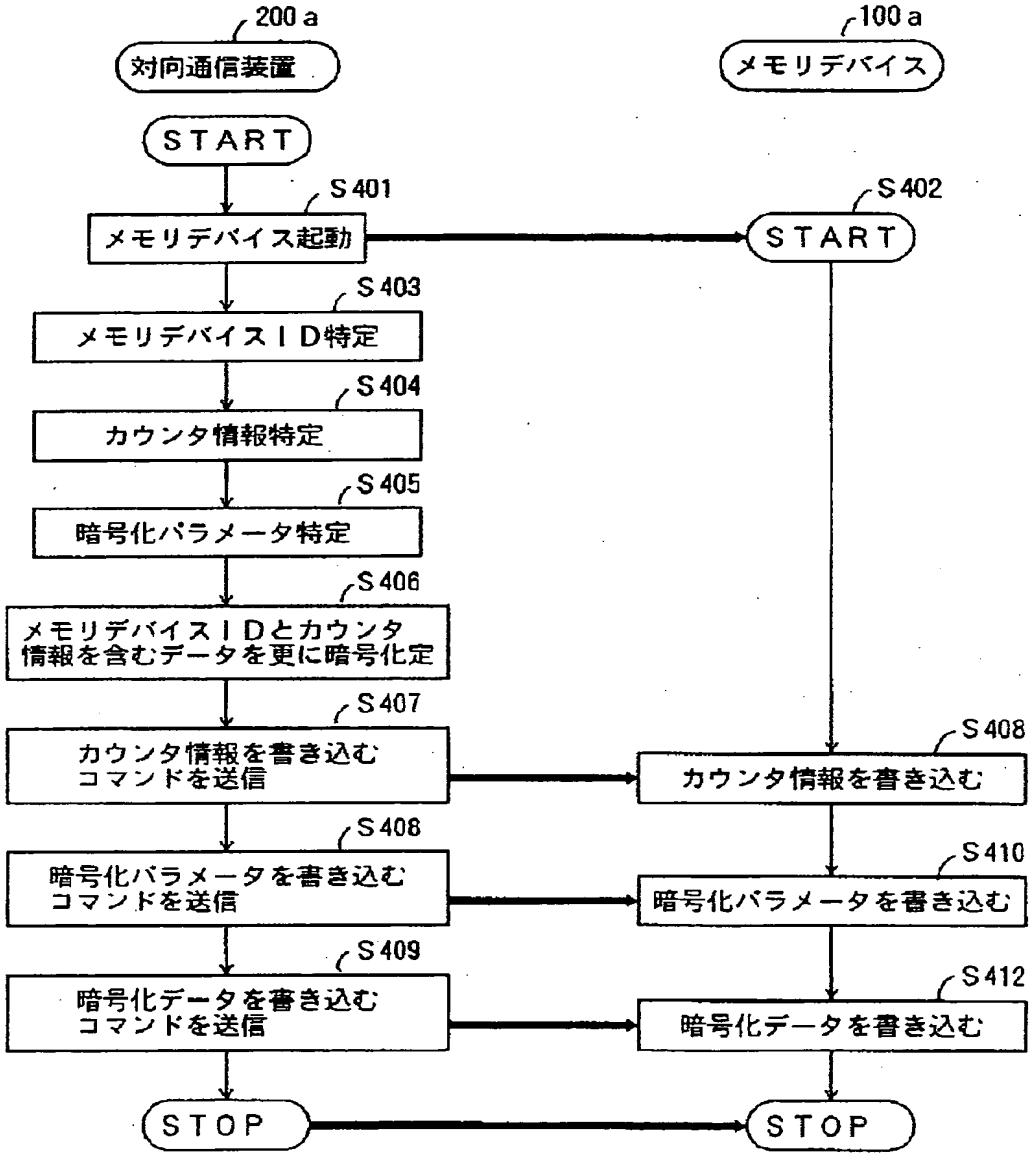
【図１６】

本発明の第３の実施例のメモリデバイスと対向通信装置が
２回目以降にやり取りする際の動作のフローチャート



【図１８】

本発明の第4の実施例のメモリデバイスと対向通信装置が最初にデータをやり取りする際の動作のフローチャート



【図１９】

本発明の第４の実施例のメモリデバイスと対向通信装置が
２回目以降にやり取りする際の動作のフローチャート